

**pkirisgrid**

**pkIRISGrid**  
**Una PKI para IRISGrid**

red.es

- Requisitos pkIRISGrid 0.2 beta – EUGridPMA
  - Cumplidos – v3.2 - 02/02/2005
- Estructura Funcional
- Tecnología usada
- Operación de la PKI
  - Capturas de pantalla
- ¿Y ahora qué?

- Requisitos pkIRISGrid 0.2 beta – EUGridPMA
  - Cumplidos – v3.2 - 02/02/2005
- Estructura
- Tecnología usada
- Operación
  - Capturas de pantalla
  - ¿Y ahora qué?

- **Controles de seguridad en la CA**
  - Máquina dedicada
  - Portatil sin tarjeta de Red
  - Descansa siempre en una caja fuerte ignífuga
  - Claves y certificados en llaves USB guardadas en la caja fuerte
- **Espacio de nombres**
  - dc=irisgrid, dc=es
    - cn=nombre@nombre, [o=nombre], dc=irisgrid, dc=es
    - cn=nombre.nombre, [o=nombre], dc=irisgrid, dc=es
- **Políticas/Documentación**
  - Política de Certificación (CP) y Prácticas de Certificación (CPS)
  - 1.3.6.1.4.1.7547.2.1.4.X - Sucesivas versiones de IRISGrid-CA
  - 1.3.6.1.4.1.7547.2.2.4.X.X - IRISGrid-CA CPS versión X.X

- **Certificados**
  - Expedirlos y revocarlos
  - Almacenar los certificados emitidos y las fechas de revocación de los mismos
  - Publicar información de revocación periódicamente
- **Revocación**
  - Solicitadas por usuario final, administrador RA y la propia CA
- **Registro de eventos**
  - Se guardan logs de todos los eventos necesarios
- **Auditorías**
  - La CA debe poder auditar a los gestores de las RAs al menos una vez al año

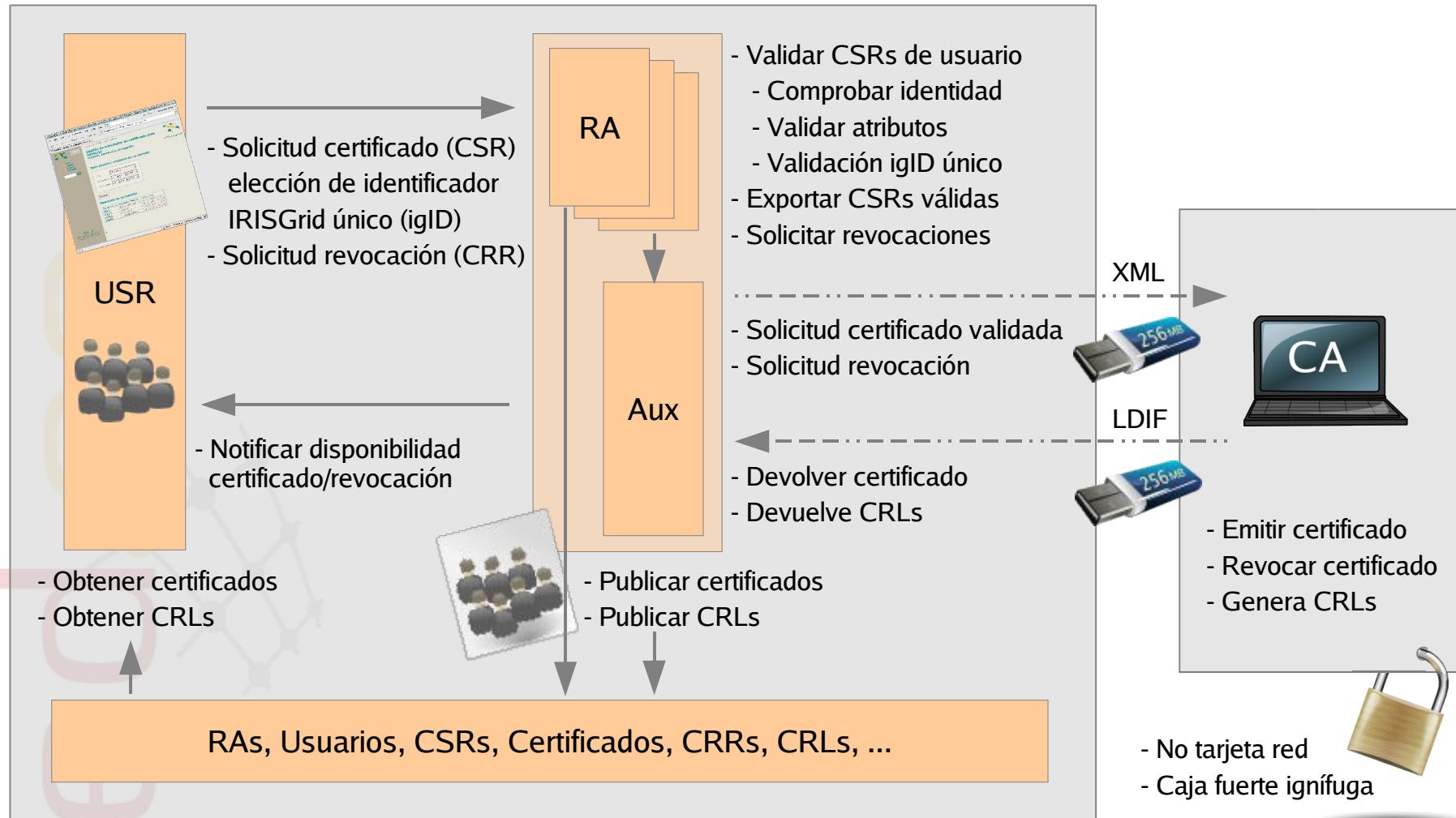
- RAs alojadas en RedIRIS (web)
  - Usuario - <http://ra1.irisgrid.es>
  - Administrador - <http://ra1.irisgrid.es/admin/>
- Identificación de entidades
  - Cada gestor/operador de RA debe conocer a sus usuarios
  - Validar identidades finales y atributos
- Unicidad en la asignación de nombres
  - No existe un sistema global de nombres que permita identificar a todo el mundo sin ambigüedad. ¿Qué tipo de nombre usamos?
  - DN: `cn=j.masa@rediris.es, dc=irisgrid, dc=es`
- Seguridad en la comunicación con la CA
  - Módulo auxiliar y llaves USB para intercambio de información

- Al estilo mail  
- NO ES MAIL



- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- **Estructura Funcional**
- Tecnología usada
  - Operación
    - Capturas de pantalla
  - ¿Y ahora qué?





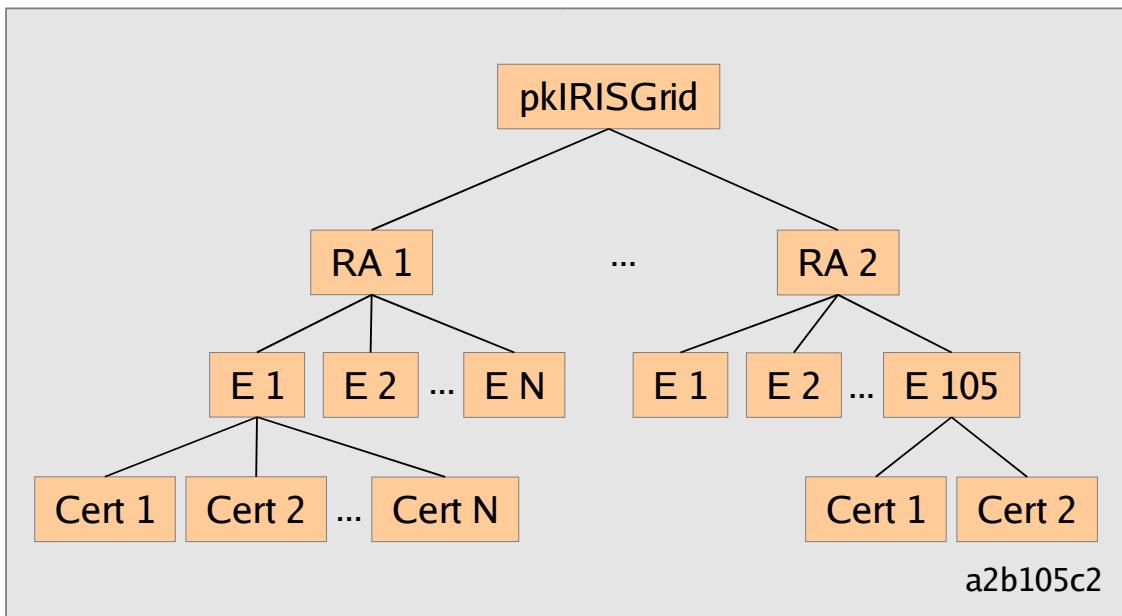
- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura
- **Tecnología usada**
  - Operación
    - Capturas de pantalla
  - ¿Y ahora qué?



- OpenSSL
- LDAP (esquema pkirisgrid)
  - Base de almacenamiento de RAs, Entidades (usuarios, servicios/servidores), CSRs, CRRs, certificados, CRLs
- COPA (Codificación optimizada para el acceso jerárquico a la información)
  - a1b105c2 identifica a RA 1, entidad 105 y a la CSR/Certificado 2
- URNs
  - Almacenamiento de histórico de estados
    - urn:mace:rediris.es:irisgrid:pki:csr:state:20050304142236:signed:10e190a0c7608fbe...2d425e6af7
- XML/LDIF
  - Ficheros de intercambio de información entre CA y RAs/Aux
- PHP (RAs), Perl (CA)
- PAPI (Control de acceso)

- **pkirisgridRA**
  - pkirisgridID
  - pkirisgridRaName
  - pkirisgridUsrCount
- **pkirisgridUsr**
  - pkirisgridID
  - cn
  - sn
  - telephoneNumber
  - mail
- **pkirisgridCert**
  - pkirisgridID
  - pkirisgridTrace
  - pkirisgridStatus
  - pkirisgridDate
  - pkirisgridPin
  - pkirisgridCSR
  - pkirisgridCertType
  - pkirisgridSubjectDN
  - userCertificate

a	Datos de las RAs
b	Datos de las entidades
c	Datos de los certificados



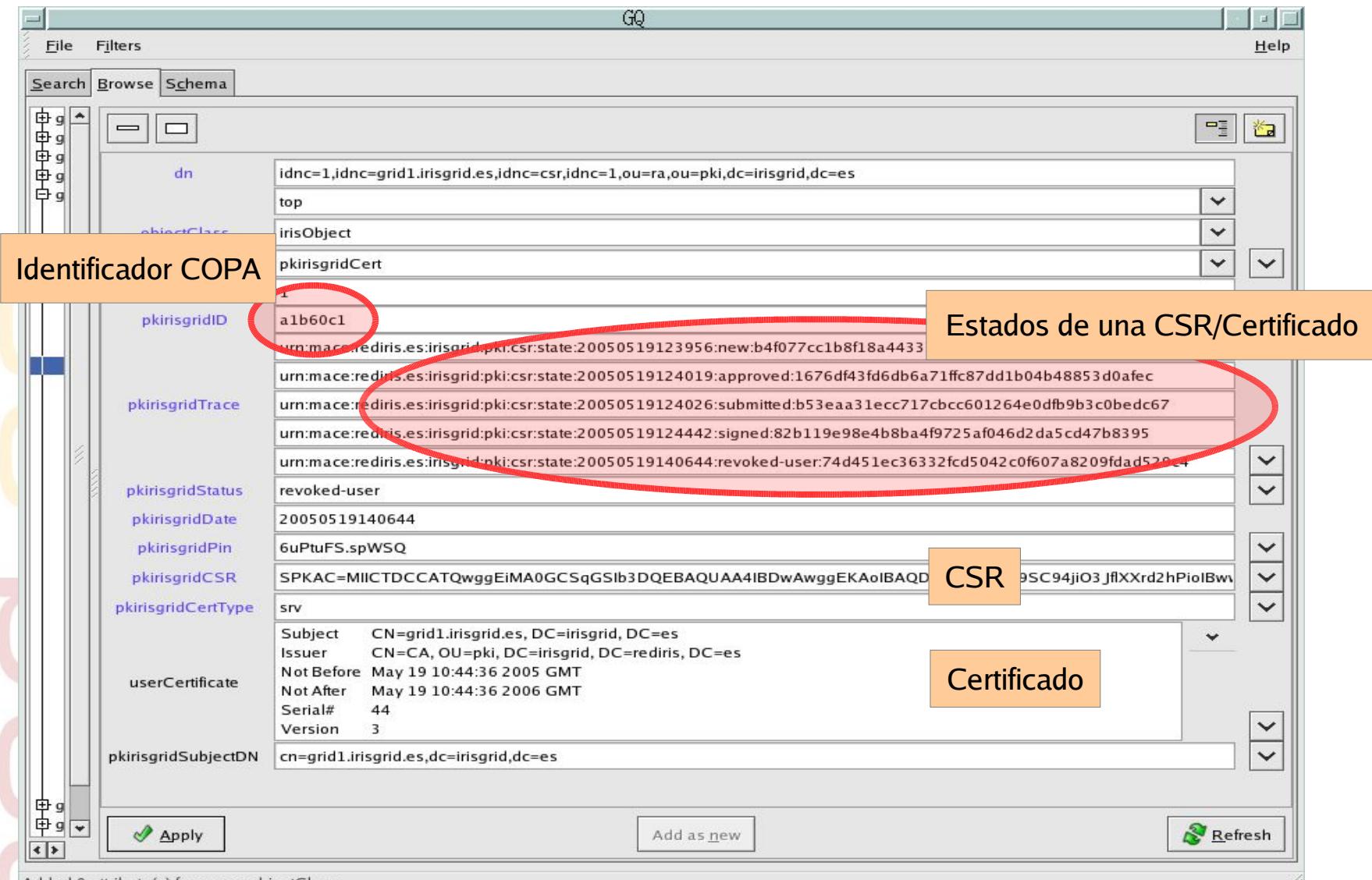
a2b105c2 identifica a la RA 2, entidad 105, y al certificado/CSR 2

Identificador COPA

Estados de una CSR/Certificado

CSR

Certificado



pkirisgridID	a1b60c1
pkirisgridTrace	urn:mace:rediris.es:irisgrid:pki:csr:state:20050519123956:new:b4f077cc1b8f18a4433 urn:mace:rediris.es:irisgrid:pki:csr:state:20050519124019:approved:1676df43fd6db6a71ffc87dd1b04b48853d0afec urn:mace:rediris.es:irisgrid:pki:csr:state:20050519124026:submitted:b53eaa31ecc717cbcc601264e0db9b3c0bedc67 urn:mace:rediris.es:irisgrid:pki:csr:state:20050519124442:signed:82b119e98e4b8ba4f9725af046d2da5cd47b8395
pkirisgridStatus	revoked-user
pkirisgridDate	20050519140644
pkirisgridPin	6uPtUFS.spWSQ
pkirisgridCSR	SPKAC=MIICDCCATQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQD9SC94jiO3JflXXrd2hPiolBwv
pkirisgridCertType	srv
userCertificate	Subject: CN=grid1.irisgrid.es, DC=irisgrid, DC=es Issuer: CN=CA, OU=pki, DC=irisgrid, DC=rediris, DC=es Not Before: May 19 10:44:36 2005 GMT Not After: May 19 10:44:36 2006 GMT Serial#: 44 Version: 3
pkirisgridSubjectDN	cn=grid1.irisgrid.es,dc=irisgrid,dc=es

Added 0 attribute(s) from new objectClass

```
<pkig>
<csrs>
<csr>
<csr_header>
<type_nav>SPKAC</type_nav>
<type_usr>usr</type_usr>
<dn>idnc=1,idnc=antonio.robles@org.es,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es</dn>
<serial>a2b2c1</serial>
<trace>urn:mace:rediris.es:irisgrid:pki:csr:state:20050307171823:approved:2b4c41234ba13 ... bde675d</trace>
</csr_header>
<csr_data>
CN = antonio.robles@org.es
1.DC = irisgrid
0.DC = es
SPKAC=MIICTDCCATQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDow69mjKY3R5/MPWuN0XW/GY
    0qF3iAUJCNZZ9Jlcz05+hpfp3g5K1E7KUE8eIW+T/eiSwC3KPH..... W+NHCr8rn/FOpoyGw==
</csr_data>
<csr_sig>c01e06d357edce49ed301bd687dae35cb520e332</csr_sig>
</csr>

<csr>
...
</csr>
</csrs>
<total_sig>7a29946e2c0a649ca31d2f530122e2b39b2f3af9</total_sig>
</pkig>
```

```
# Fichero LDIF para volcar a la CA de la pkirisgrid
# Usuario: antonio.robles@org.es
dn: idnc=1,idnc=antonio.robles@org.es,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: signed

replace: pkirisgridDate
pkirisgridDate: 20050230131552
-
add: pkirisgridTrace
pkirisgridTrace: urn:mace:rediris.es:irisgrid:pki:csr:state:20050230131552:signed:86fc84c4778e38 ... 46fc52198adc
-
replace: userCertificate:binary
userCertificate;binary::MIIFGDCCBACgAwIBAgIBFjANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQDEwJAoGA1UE
EAYKCZImiZPyLGQBGRMCZXMuHhcNMDUwMzMwMTExNTUxWhcNMDYwMzMwMTExNTUxWjBpMRIwEAYD
.....
K4Q3AKwSVVxlykqycV059KJN2MDJWIpur2+/FwjkUyrXJwUG5kLPyPu7Jnxd4k54ifpQKJB7NVXu
HkM549/gD9zVlkY9jAKCzKpkkXgF4ghRcMvNAS7OCs/Z4N8MNzSsOVsArD3XNXGcG+0l7Kop
```

```
#Usuario: towoto2.firefox@rediris.es
dn: idnc=1,idnc=towoto2.firefox@rediris.es,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: signed
.....
```



```
<pkig>
<crr_header>
<crt_igID>a2b4c1</crt_igID>
<crt_serial>22</crt_serial>
<csr_dn>idnc=1,idnc=ww@ww.com,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es</csr_dn>
<crr_ra>2</crr_ra>
<crr_user>user</crr_user>
</crr_header>
<crr>
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 22 (0x16)
Signature Algorithm: sha1WithRSAEncryption
Issuer: CN=CA, OU=pki, DC=irisgrid, DC=es
Validity
Not Before: Mar 30 11:15:51 2005 GMT
Not After : Mar 30 11:15:51 2006 GMT
Subject: CN=ww@ww.com, DC=irisgrid, DC=es
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:b8:ad:27:8e:03:95:b8:c6:18:0f:73:e2:df:b4:
6d:be:f5:2f:4c:b9:88:36:84:79:f5:93:6b:60:90:
...
-----END CERTIFICATE-----
</crr>
<sig>61479b34d197f5d2461da22dbf0b9c4112557a49</sig>
</pkig>
```

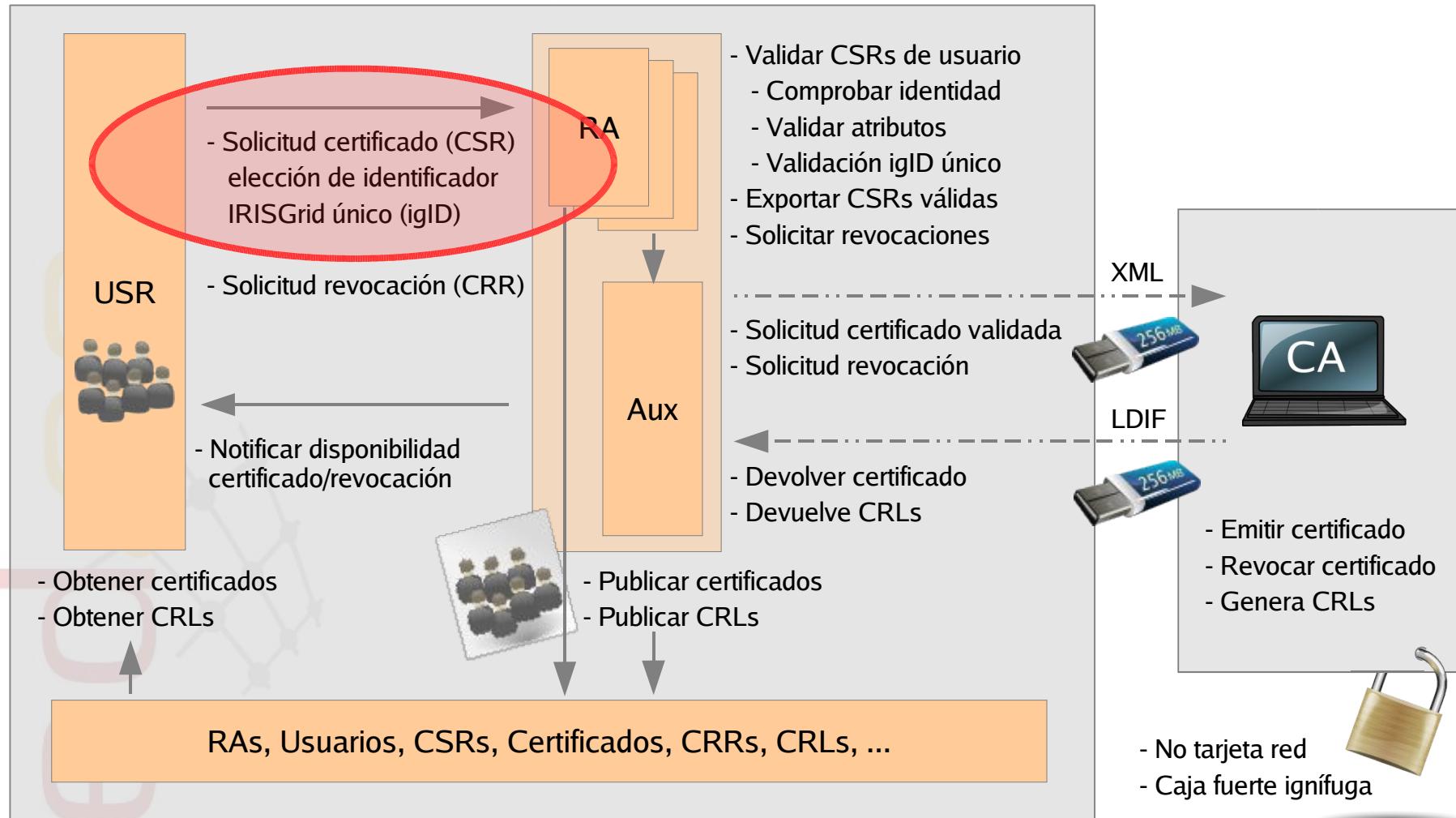


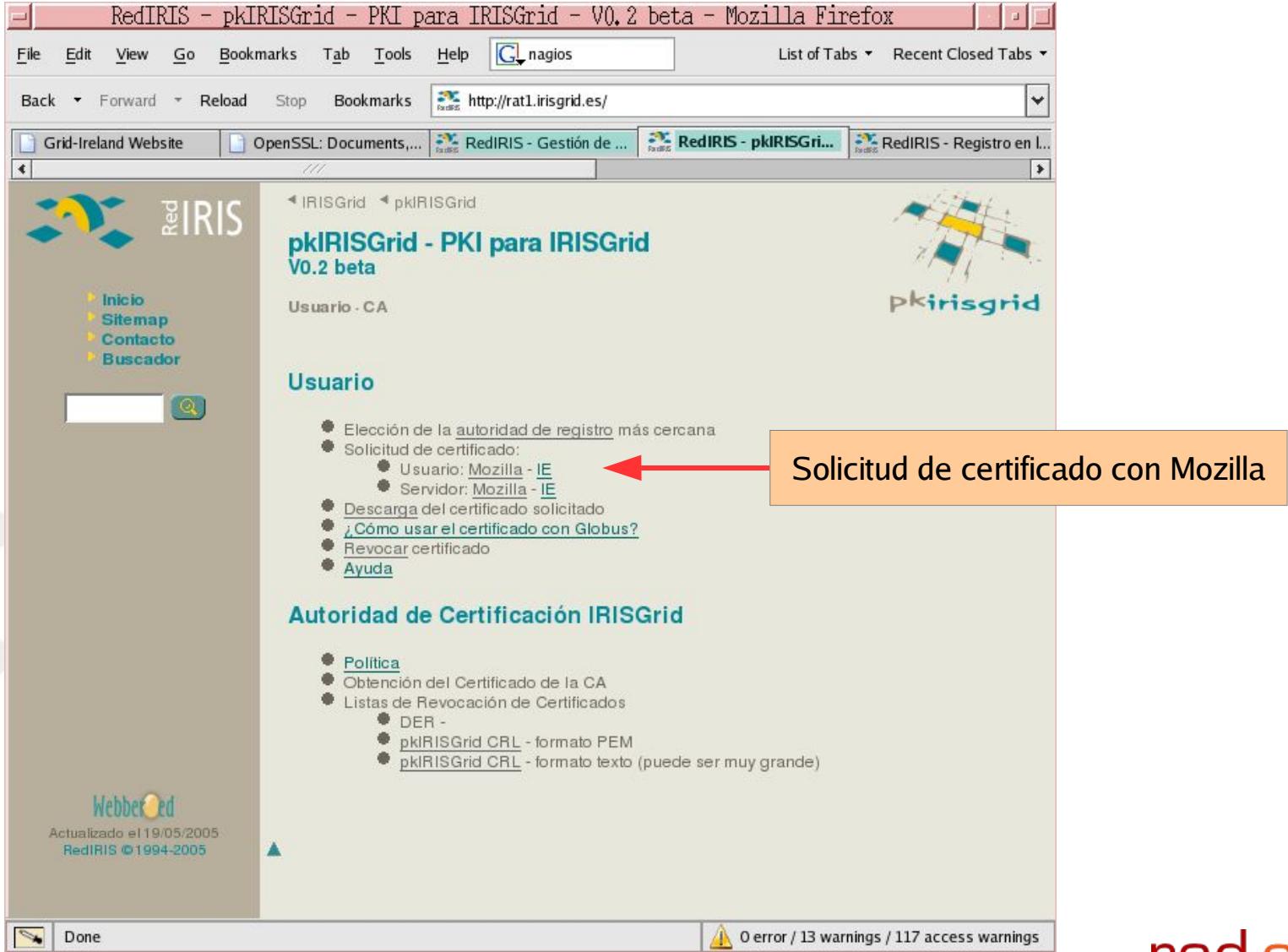
```
dn: idnc=1,idnc=ww@ww.com,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: revoked-user
-
replace: pkirisgridDate
pkirisgridDate: 20050304142236
-
add: pkirisgridTrace
pkirisgridTrace: urn:mace:rediris.es:irisgrid:pki:csr:state:20050304142236:
revoked-user:10e190a0c760 8fbe2d4...5f2ec57
```



- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura
- Tecnología usada
- **Operación**
  - Capturas de pantalla
  - ¿Y ahora qué?







The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** RedIRIS - pkIRISGrid - PKI para IRISGrid - V0.2 beta - Mozilla Firefox
- Address Bar:** http://rat1.irisgrid.es/
- Toolbar:** File, Edit, View, Go, Bookmarks, Tab, Tools, Help.
- Tab Bar:** Grid-Ireland Website, OpenSSL: Documents..., RedIRIS - Gestión de ..., RedIRIS - pkIRISGrid..., RedIRIS - Registro en I...
- Content Area:**
  - Left Sidebar:** RedIRIS logo, Inicio, Sitemap, Contacto, Buscador, Webbered logo, Actualizado el 19/05/2005, RedIRIS ©1994-2005.
  - Main Content:**
    - Section:** pkIRISGrid - PKI para IRISGrid V0.2 beta
    - User Section:** Usuario . CA
    - Section:** Usuario
      - Elección de la autoridad de registro más cercana
      - Solicitud de certificado:
        - Usuario: Mozilla - IE
        - Servidor: Mozilla - IE
      - Descarga del certificado solicitado
      - [¿Cómo usar el certificado con Globus?](#)
      - Revocar certificado
      - Ayuda
    - Section:** Autoridad de Certificación IRISGrid
      - Política
      - Obtención del Certificado de la CA
      - Listas de Revocación de Certificados
        - DER -
        - [pkIRISGrid CRL](#) - formato PEM
        - [pkIRISGrid CRL](#) - formato texto (puede ser muy grande)

Solicitud de certificado con Mozilla

The screenshot shows a Mozilla Firefox browser window with the title "RedIRIS - Solicitud de certificado de usuario para IRISGrid - para Mozilla y compatibles". The URL is "http://rat1.irisgrid.es/csr\_spkac\_usr.phtml". The page displays a form for a user certificate request. The "Identificador IRISGrid" field contains "j.masa" followed by a dropdown menu showing "rediris.es", "rediris.com", and "irisgrid.es". The "email" field contains "javi@no-spam.es". The "PIN" and "Repite PIN" fields both contain "\*\*\*\*\*". A red arrow points from the text "Identificador IRISGrid nombre@org.dom" to the dropdown menu. Another red arrow points from the text "PIN muy importante para las revocaciones" to the PIN fields.

Identificador IRISGrid  
nombre@org.dom

j.masa@rediris.es

PIN muy importante  
para las revocaciones

Continuar

Done

0 error / 18 warnings / 138 access warnings

RedIRIS - Solicitud de certificado de usuario para IRISGrid - para Mozilla y compatibles

File Edit View Go Bookmarks Tab Tools Help G nagios List of Tabs Recent Closed Tabs

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.es/csr\_spkac\_usr.phtml

Grid-Ireland Website OpenSSL: Documents,... RedIRIS - Gestión de ... RedIRIS - Solicitud ... RedIRIS - Registro en I...

IRISGrid pkIRISGrid

Solicitud de certificado de usuario para IRISGrid para Mozilla y compatibles (SPKAC)

Detalles de la solicitud

Subject DN: cn=j.masa@rediris.es,o=rediris.es,dc=irisgrid,dc=es

Identificador IRISGrid	j.masa@rediris.es
Nombre	Javier Masa Marin
Mail	javi@no-spam.es
Teléfono	955123123123

OJO: Revisar datos

Tamaño de la clave (se recomienda 2048 bits)

2048 (High Grade) ▾ Continuar

Tamaño clave 2048

Done 0 error / 16 warnings / 140 access warnings

# pkIRISGrid v0.2 beta

## Solicitud de certificado aceptada

RedIRIS - Solicitud de Certificado para IRISGrid - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help G

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/csr\_add.phtml

RedIRIS - Solicitud de Certificado para I...

IRISGrid pkIRISGrid

Solicitud de Certificado para IRISGrid

pkirisgrid

Solicitud aceptada

Su solicitud:

- Identificador IRISGrid: j.masa@rediris.es
- Código solicitud: a1b33c1

ha sido aceptada

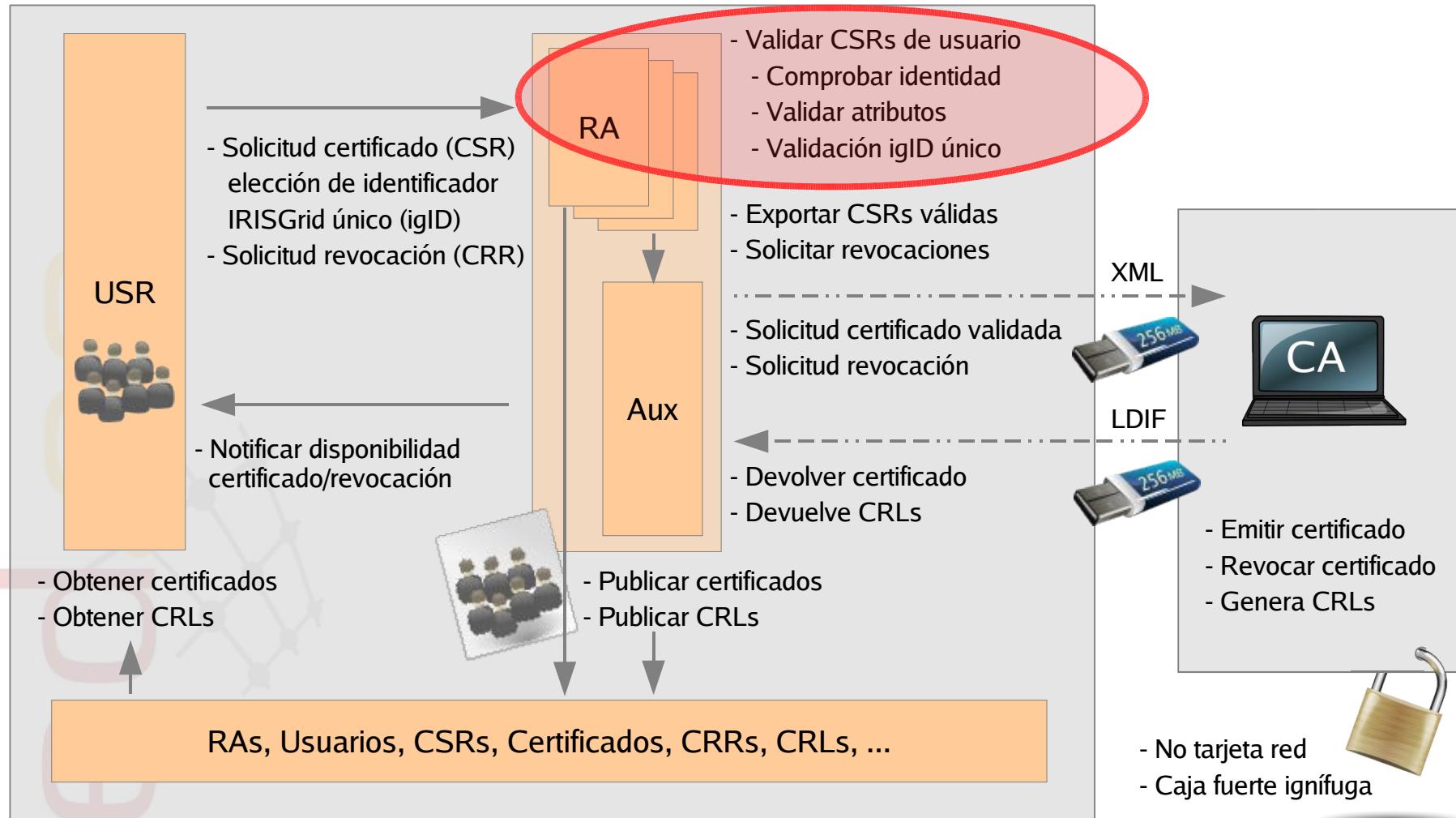
Por favor, es muy importante que anote los valores anteriores ya que las siguientes operaciones:

- Autenticación frente a la autoridad de registro
- Descarga de su certificado
- Revocación de su certificado

igID: j.masa@rediris.es

código CSR: a1b33c1

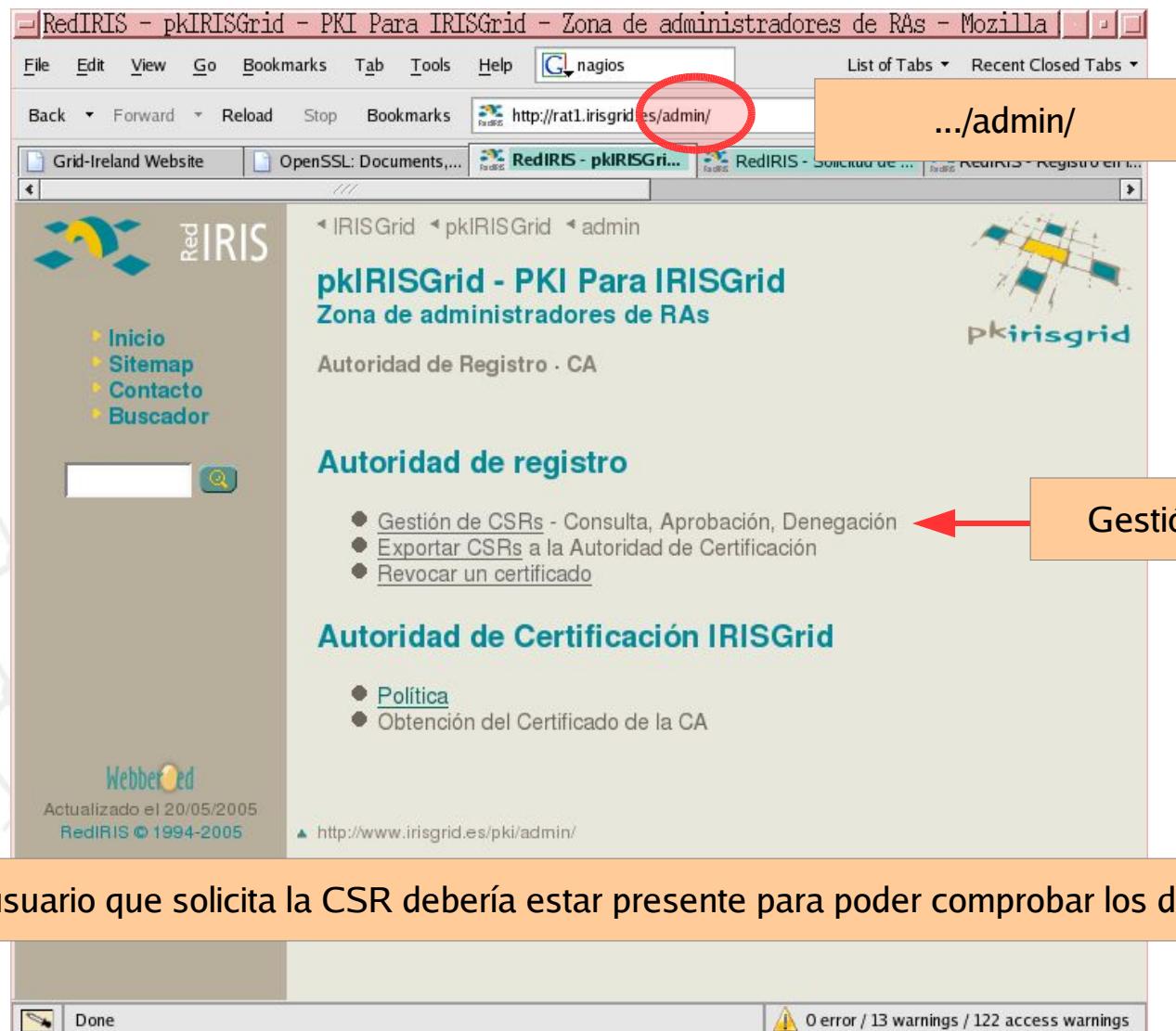
Done 0 error / 17 warnings / 111 access warnings



RAs, Usuarios, CSRs, Certificados, CRRs, CRLs, ...



S  
E  
O  
C  
E  
D  
E  
R  
E  
D  
A  
S



RedIRIS - pkIRISGrid - PKI Para IRISGrid - Zona de administradores de RAs - Mozilla

File Edit View Go Bookmarks Tab Tools Help nagios

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.es/admin/ List of Tabs Recent Closed Tabs

Grid-Ireland Website OpenSSL: Documents... RedIRIS - pkIRISGrid RedIRIS - Solicitud de ... RedIRIS - Registro en ...

.../admin/

IRISGrid pkIRISGrid admin

**pkIRISGrid - PKI Para IRISGrid**  
Zona de administradores de RAs

Autoridad de Registro · CA

**Autoridad de registro**

- [Gestión de CSRs](#) - Consulta, Aprobación, Denegación
- [Exportar CSRs](#) a la Autoridad de Certificación
- [Revocar un certificado](#)

**Autoridad de Certificación IRISGrid**

- [Política](#)
- Obtención del Certificado de la CA

▲ http://www.irisgrid.es/pki/admin/

El usuario que solicita la CSR debería estar presente para poder comprobar los datos

Done 0 error / 13 warnings / 122 access warnings

RedIRIS - Gestión de solicitudes de certificado para IRISGrid - Consulta, Aprobación, Denegación

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/csr\_search.phtml

RedIRIS - Gestión de solicitudes de certificado para IRISGrid

IRISGrid < pkIRISGrid < admin

Gestión de solicitudes de certificado para IRISGrid  
Consulta, Aprobación, Denegación

pkirisgrid

Selección de los requisitos de su consulta

Tipo: CSR Nueva

Fecha desde: 1 1 2005

Fecha hasta: 31 12 2010

Continuar

CSRs Nuevas

Resultado de su consulta

Código solicitud	Identificador IRISGrid	Fecha evento
a1b4c1	diego.lopez@rediris.es	24 / 02 / 2005 - 12:28:41
a1b31c1	a@a.com	16 / 03 / 2005 - 17:07:56
a1b32c1	ee@ee.com	16 / 03 / 2005 - 17:44:30
a1b33c1	j.masa@rediris.es	05 / 04 / 2005 - 7:49:18

a1b33c1 - j.masa@rediris.es

Done

0 error / 23 warnings / 136 access warnings

RedIRIS - Gestión de solicitudes de certificado para IRISGrid - Operaciones disponibles

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/csr\_manage.phtml

RedIRIS - Gestión de solicitudes de cert...

IRISGrid pkIRISGrid admin

Gestión de solicitudes de certificado para IRISGrid  
Operaciones disponibles para una solicitud

pkirisgrid

Detalles de la solicitud

Autoridad de registro	RedIRIS
Número serie	a1b33c1
Identificador IRISGrid	j.masa@rediris.es
Nombre	Javier Masa Marin
Mail	javi@spamno.es
Teléfono	95505111111
Fecha solicitud	06/04/2005 - 17:49:18
Estado solicitud	<b>new</b>

Comprobar identidad  
Comprobar datos

Estado: Nueva

Verificar PIN

Aprobar solicitud Borrar solicitud

JavaScript Application

¿Está seguro de aprobar esta solicitud?

Cancel OK

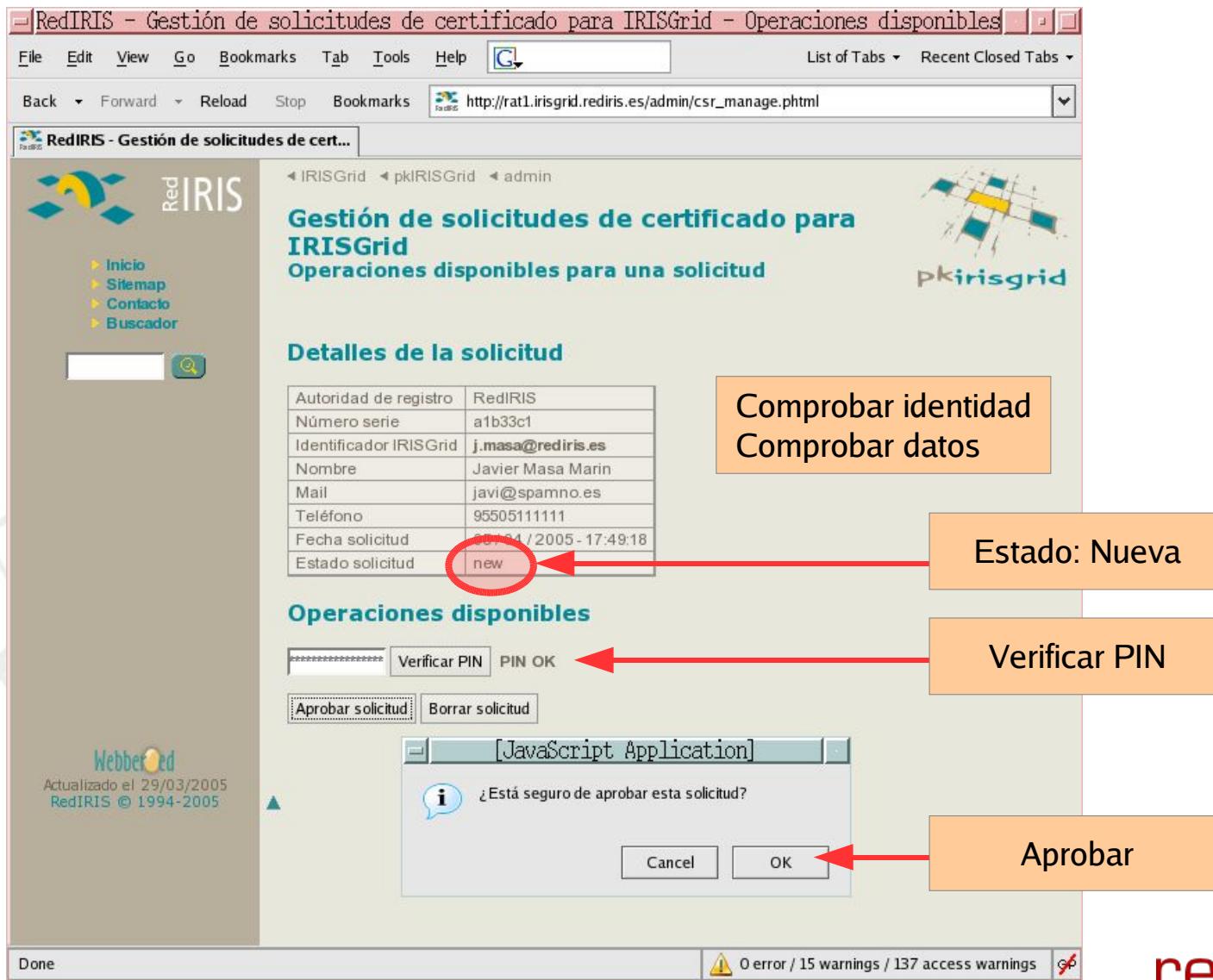
Aprobar

Done

0 error / 15 warnings / 137 access warnings

red.es

pkirisgrid



# pkIRISGrid v0.2 beta

## Resultado de la aprobación

RedIRIS - Gestión de solicitudes de certificado para IRISGrid - Operaciones disponibles

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/csr\_manage.phtml

RedIRIS - Gestión de solicitudes de cert...

IRISGrid pkIRISGrid admin

Gestión de solicitudes de certificado para IRISGrid Operaciones disponibles para una solicitud

pkirisgrid

Resultado de la solicitud

Su solicitud ha sido procesada

Detalles de la solicitud

Autoridad de registro	RedIRIS
Número serie	a1b33c1
Identificador IRISGrid	j.masa@rediris.es
Nombre	Javier Masa Marin
Mail	javi@spamno.es
Teléfono	95505111111
Fecha solicitud	05/05/2005 - 17:54:02
Estado solicitud	approved

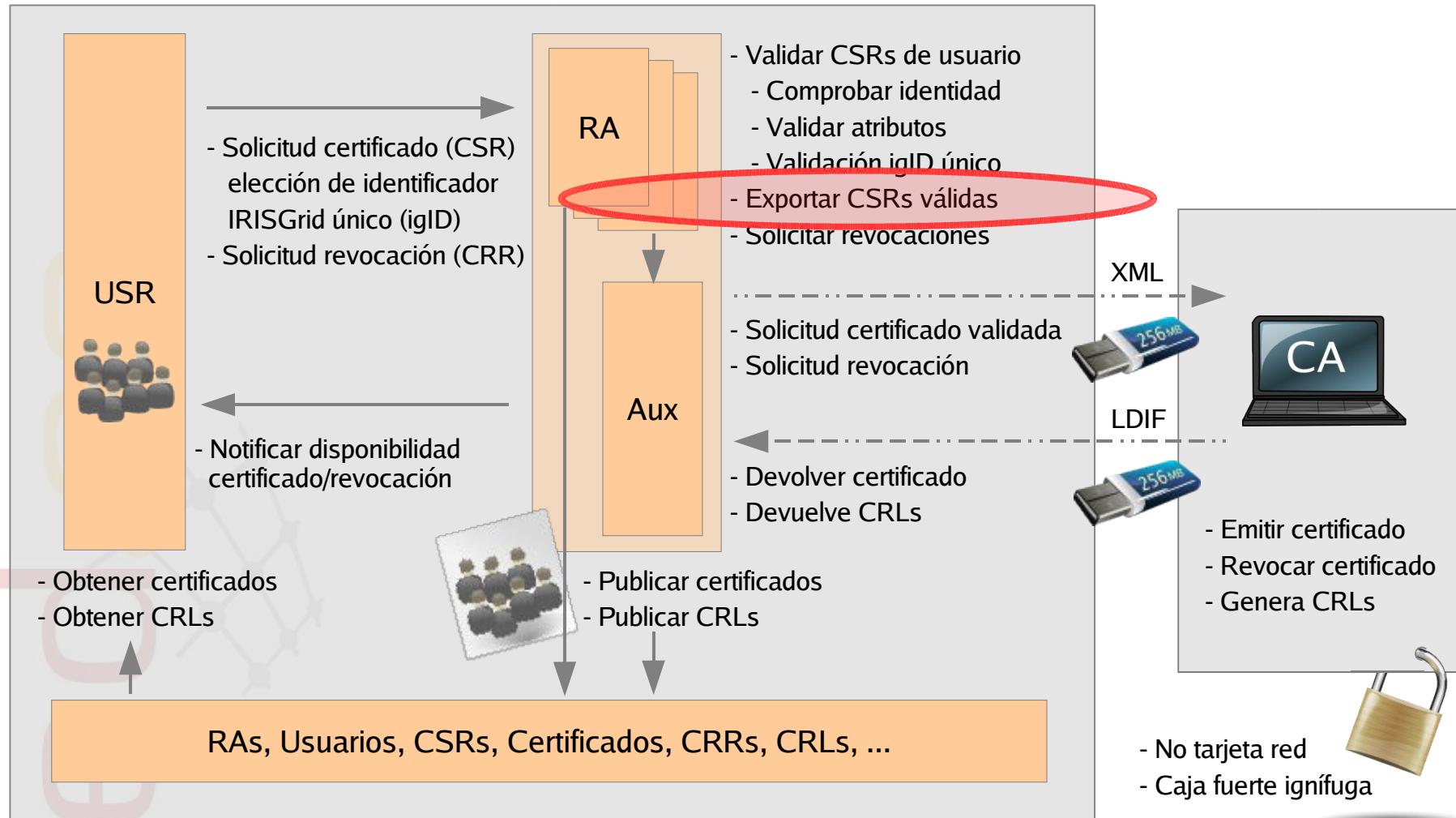
Estado: Aprobada

Operaciones disponibles

Ninguna

Done

0 error / 15 warnings / 131 access warnings



RedIRIS - pkIRISGrid - PKI Para IRISGrid - Zona de administradores de RAs - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help  nagios List of Tabs Recent Closed Tabs

Back Forward Reload Stop Bookmarks <http://rat1.irisgrid.es/admin/>

Grid-Ireland Website OpenSSL: Documents,... RedIRIS - pkIRISGrid RedIRIS - Solicitud de ... RedIRIS - Registro en I...

IRISGrid pkIRISGrid admin

**pkIRISGrid - PKI Para IRISGrid**  
Zona de administradores de RAs

Autoridad de Registro . CA

**Autoridad de registro**

- Gestión de CSRs - Consulta, Aprobación, Denegación
- Exportar CSRs a la Autoridad de Certificación** 
- Revocar un certificado

**Exportar CSRs validadas**

**Autoridad de Certificación IRISGrid**

- Política
- Obtención del Certificado de la CA

Actualizado el 20/05/2005  
RedIRIS © 1994-2005

Done 0 error / 13 warnings / 122 access warnings



# pkIRISGrid v0.2 beta

## Listado de CSRs a exportar a la CA

RedIRIS - Exportación de las CSRs - a la Autoridad de Certificación IRISGrid - Mozilla

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/csr\_export.phtml

RedIRIS - Exportación de las CSRs - a la...

IRISGrid pkIRISGrid admin

**Exportación de las CSRs  
a la Autoridad de Certificación IRISGrid**

CSRs que se van a enviar a la CA

Código solicitud	Identificador IRISGrid	Fecha
a1b33c1	j.masa@rediris.es	05 / 04 / 2005 - 17:54:02

Enviar a la CA

Done

0 error / 24 warnings / 131 access warnings



# pkIRISGrid v0.2 beta

## Resultado de la exportación de CSRs

RedIRIS - Exportación de las CSRs - a la Autoridad de Certificación IRISGrid - Mozilla

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/csr\_export.phtml

RedIRIS - Exportación de las CSRs - a la...

IRISGrid < pkIRISGrid < admin

**Exportación de las CSRs  
a la Autoridad de Certificación IRISGrid**

pkirisgrid

Hay 1 CSRs que se van a enviar a la CA

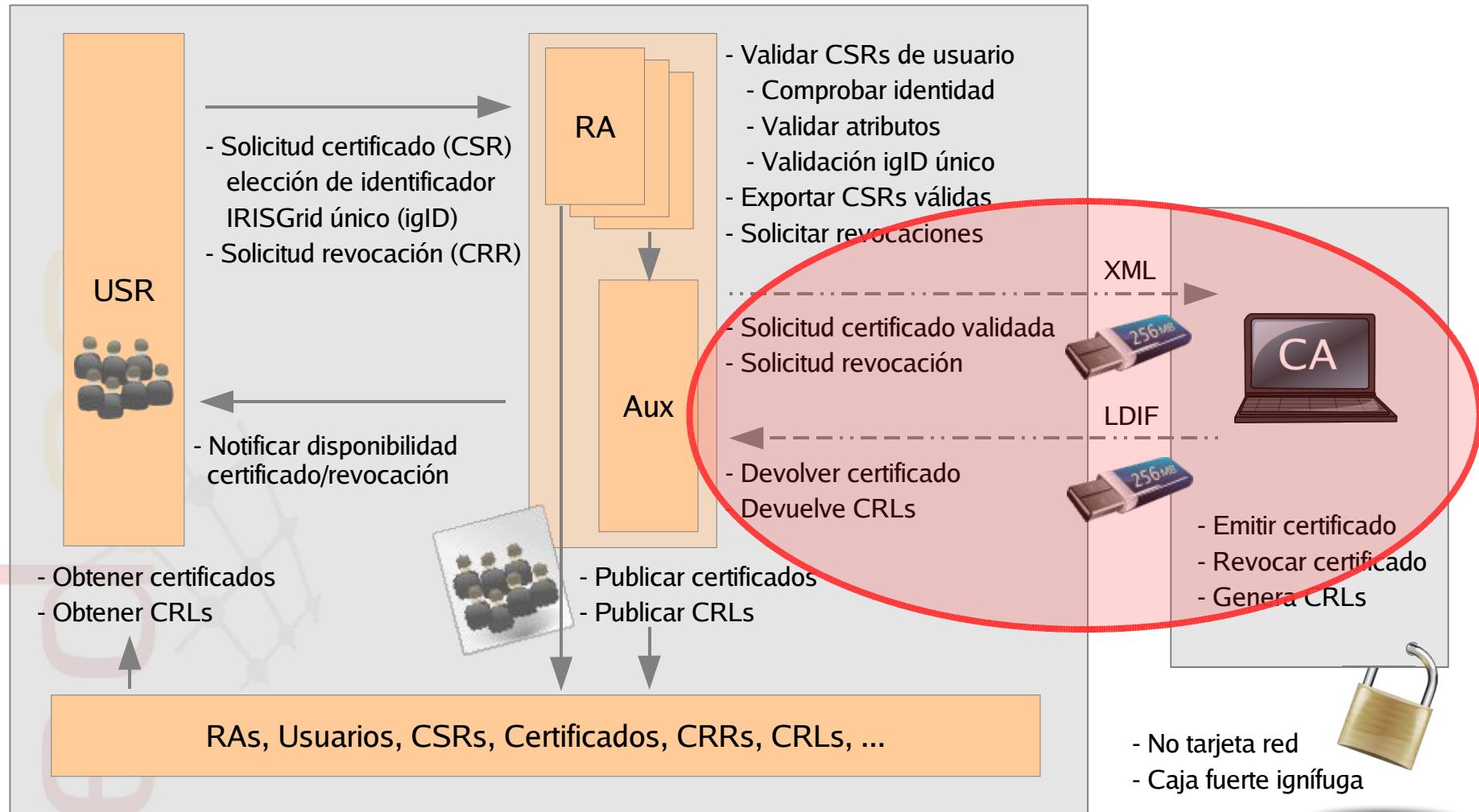
La exportación de las CSRs se ha realizado con éxito

Webbered

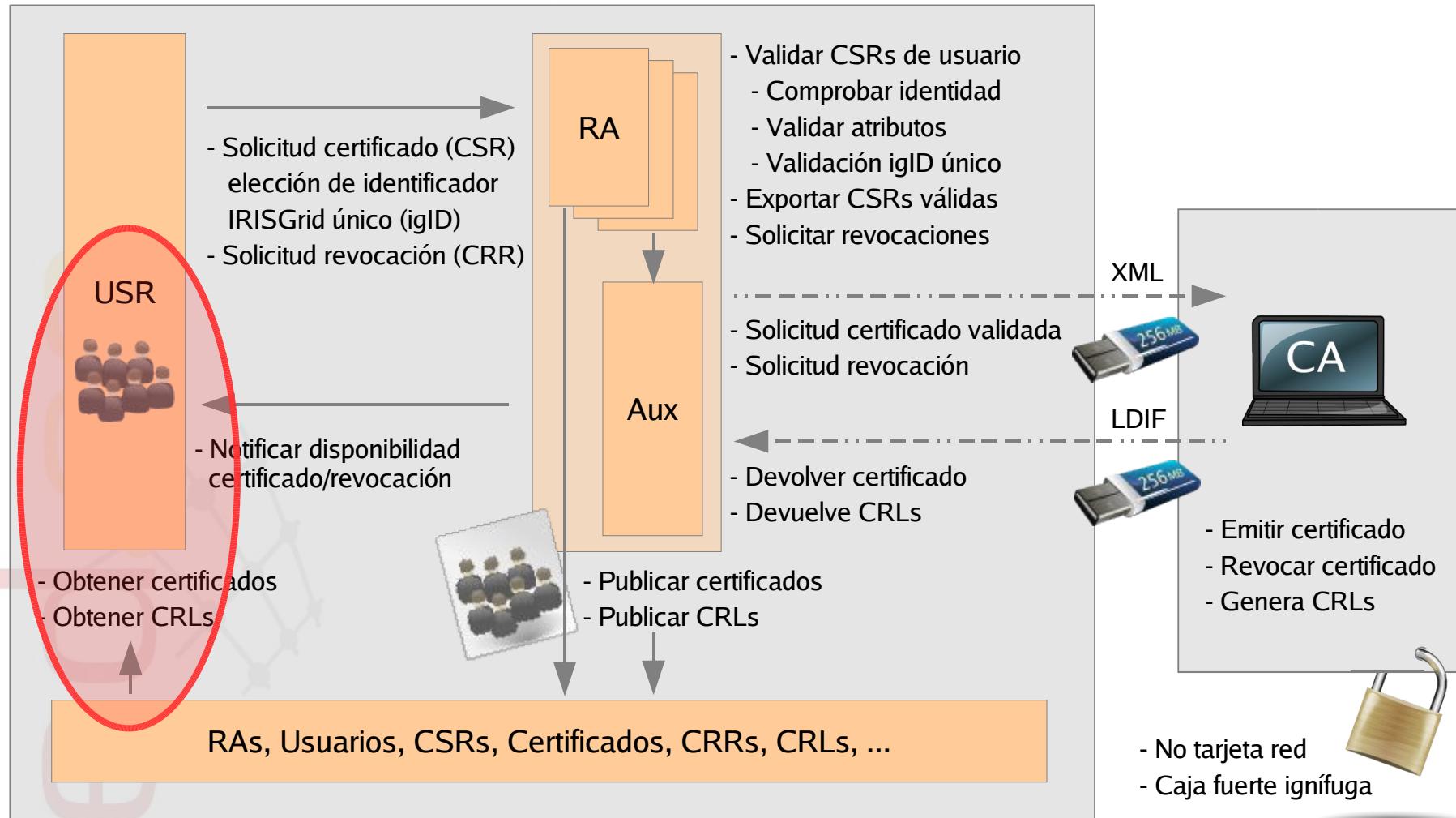
Actualizado el 30/03/2005  
RedIRIS © 1994-2005

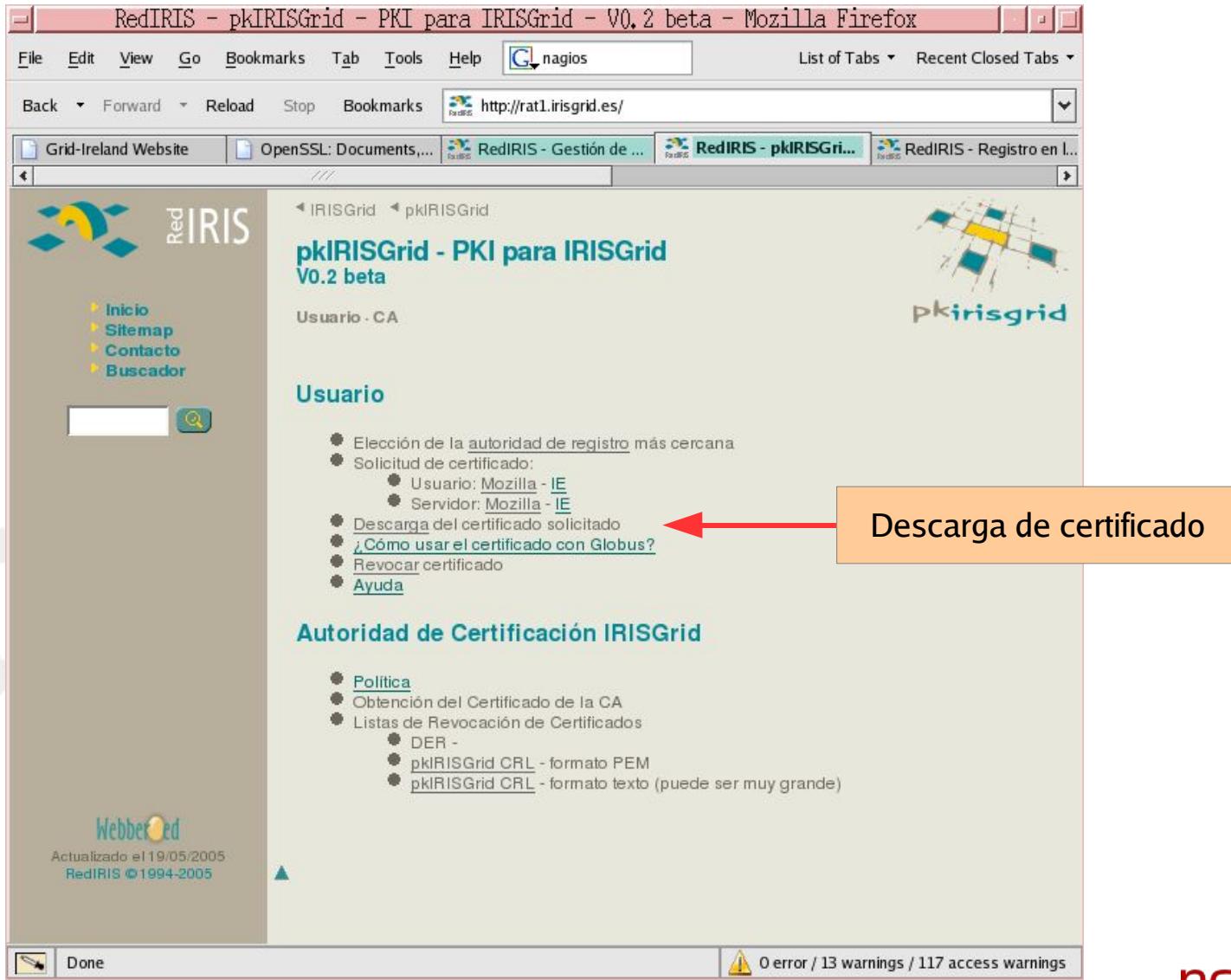
Done

⚠ 0 error / 15 warnings / 120 access warnings



- Operador CA recibe las CSRs, CRRs
  - por mail, ftp, ... en formato XML
- Exporta esos ficheros XML a una llave USB
- Saca la CA del armario, la enciende y monta la llave USB
- Ejecuta el programa correspondiente (ca, crr, crl, ...)
  - Firma, Revoca, Genera CRL, ... y obtiene salidas LDIF
- Copia esos ficheros a la llave USB
- Desmonta la llave USB, apaga el PC y **lo guarda**
- Lleva la llave USB a un PC con acceso a la red
- Vuelca al LDAP todos los ficheros LDIF
  - Se actualizan los certificados, CRLs, trazas, ...





RedIRIS - pkIRISGrid - PKI para IRISGrid - V0.2 beta - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help C nagios

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.es/

Grid-Ireland Website OpenSSL: Documents... RedIRIS - Gestión de ... RedIRIS - pkIRISGrid... RedIRIS - Registro en l...

 RedIRIS

IRISGrid pkIRISGrid

**pkIRISGrid - PKI para IRISGrid**  
V0.2 beta

Usuario . CA

**Usuario**

- Elección de la autoridad de registro más cercana
- Solicitud de certificado:
  - Usuario: Mozilla - IE
  - Servidor: Mozilla - IE
- Descarga del certificado solicitado
- Cómo usar el certificado con Globus?
- Revocar certificado
- Ayuda

**Autoridad de Certificación IRISGrid**

- Política
- Obtención del Certificado de la CA
- Listas de Revocación de Certificados
  - DER -
  - pkIRISGrid CRL - formato PEM
  - pkIRISGrid CRL - formato texto (puede ser muy grande)

Done 0 error / 13 warnings / 117 access warnings

Descarga de certificado

# pkIRISGrid v0.2 beta

## Selección del certificado

RedIRIS - Descarga del certificado solicitado para IRISGrid - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/crt\_get.phtml

List of Tabs Recent Closed Tabs

RedIRIS - Descarga del certificado soliciti...

IRISGrid pkIRISGrid

Descarga del certificado solicitado para IRISGrid

pkirisgrid

Introduzca los siguientes datos

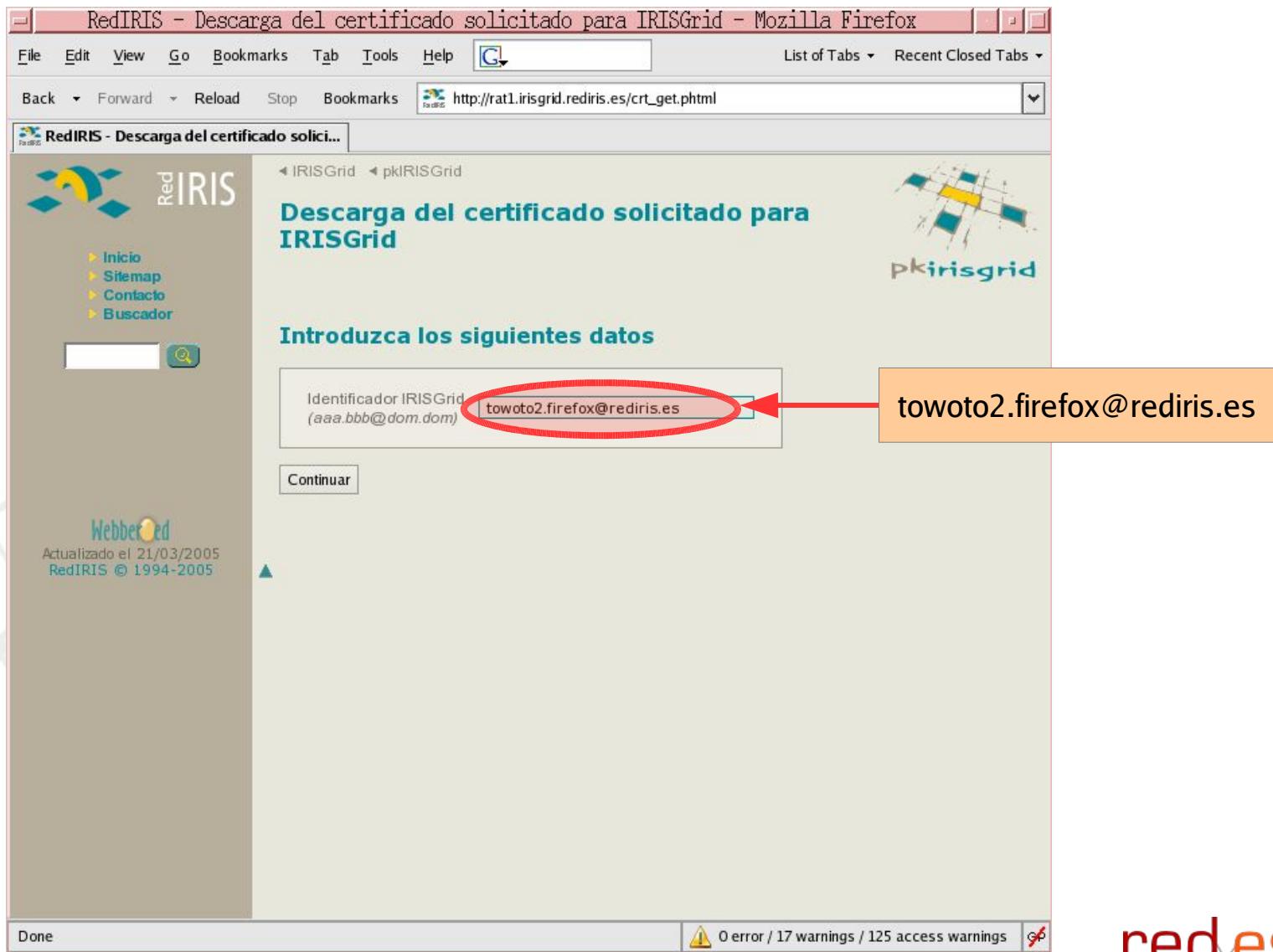
Identificador IRISGrid  
(aaa.bbb@dom.dom) towoto2.firefox@rediris.es

Continuar

towoto2.firefox@rediris.es

Done

0 error / 17 warnings / 125 access warnings



# pkIRISGrid v0.2 beta

## Comprobación de datos del certificado

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** RedIRIS - Descarga del certificado solicitado para IRISGrid - Mozilla Firefox
- Address Bar:** http://rat1.irisgrid.rediris.es/crt\_get.phtml
- Page Content:**
  - Header:** RedIRIS - Descarga del certificado solicitado...
  - Left Sidebar:** RedIRIS logo, navigation links (Inicio, Sitemap, Contacto, Buscador), and a search bar.
  - Main Content:**
    - Section:** Descarga del certificado solicitado para IRISGrid
    - Section:** Datos sobre la solicitud del certificado (CSR)

Identificador IRISGrid	towoto2.firefox@rediris.es
Nombre	towoto firefox
Número de serie de la CSR	a1b24c1
    - Note:** Para instalar el certificado en su navegador es necesario que utilice el mismo navegador desde el que realizó la petición del certificado. En caso contrario no podrá instalarlo.
    - Buttons:** Instalar su certificado en el navegador (circled in red) and Instalar el certificado.
    - Section:** Datos sobre el certificado que va a descargar
    - Text:** Issuer: CN=CA, OU=pki, DC=irisgrid, DC=es  
Subject: CN=towoto2.firefox@rediris.es, DC=irisgrid, DC=es
    - Text:** Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public Key: (1024 bit)  
Modulus (1024 bit):  
00:cb:22:c5:ae:56:2f:cc:8f:8c:6a:1a:98:99:c3:  
d9:1f:bc:f4:5e:71:ec:c9:ad:e6:68:f5:d3:b1:5a:  
c3:83:65:f8:e7:50:80:ea:76:44:95:52:e1:8a:fe:  
7a:13:96:78:75:cf:2b:12:39:a1:2f:17:0a:cd:c1:  
... (truncated)

RedIRIS - Descarga del certificado solicitado para IRISGrid - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/crt\_get.phptml

RedIRIS - Descarga del certificado solici...

IRISGrid pkIRISGrid

**Descarga del certificado solicitado para IRISGrid**

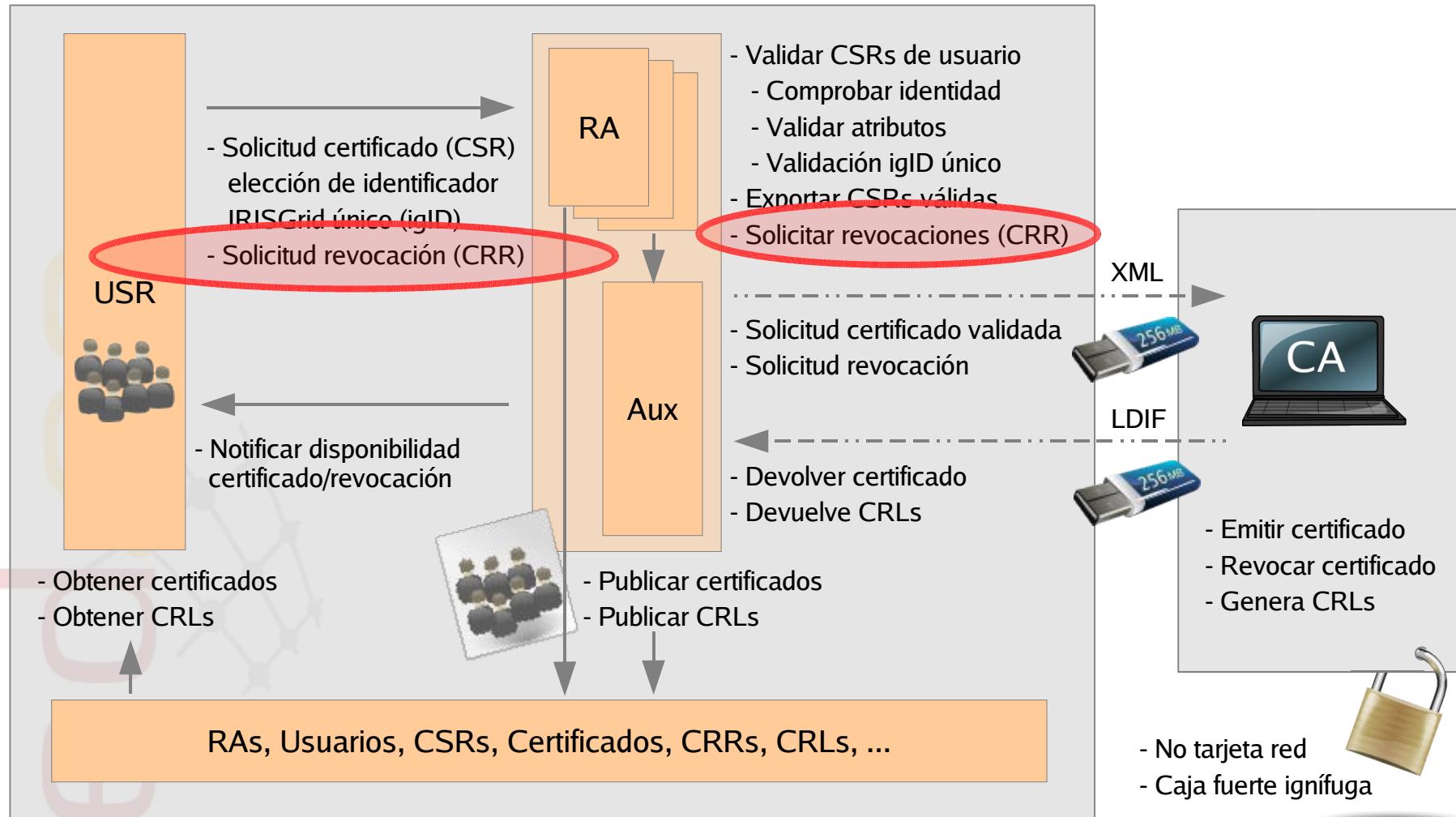
**Certificado descargado**

Su certificado ha sido instalado en su navegador si está utilizando el mismo navegador desde el que solicitó la petición de certificado

Por favor, compruebe en las preferencias de su navegador si el certificado se encuentra instalado en la base de datos de certificados personales

Actualizado el 21/03/2005  
RedIRIS © 1994-2005

Done 0 error / 15 warnings / 119 access warnings



RAs, Usuarios, CSRs, Certificados, CRRs, CRLs, ...

- No tarjeta red
- Caja fuerte ignífuga



RedIRIS - pkIRISGrid - PKI Para IRISGrid - Zona de administradores de RAs - Mozilla

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.es/admin/

Grid-Ireland Website OpenSSL: Documents,... RedIRIS - pkIRISGrid... RedIRIS - Solicitud de ... RedIRIS - Registro en L...

IRISGrid pkIRISGrid admin

**pkIRISGrid - PKI Para IRISGrid**  
Zona de administradores de RAs

Autoridad de Registro . CA

**Autoridad de registro**

- Gestión de CSRs - Consulta, Aprobación, Denegación
- Exportar CSRs a la Autoridad de Certificación
- Revocar un certificado

**Revocar certificado**

**Autoridad de Certificación IRISGrid**

- Política
- Obtención del Certificado de la CA

Actualizado el 20/05/2005  
RedIRIS © 1994-2005

http://www.irisgrid.es/pki/admin/

Done 0 error / 13 warnings / 122 access warnings

RedIRIS - Solicitud de revocación de certificado para IRISGrid - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/crr.phtml

RedIRIS - Solicitud de revocación de cer...

IRISGrid pkIRISGrid admin

Solicitud de revocación de certificado para IRISGrid

pkirisgrid

Introduzca los siguientes datos

Identificador IRISGrid (nombre@org)  j.masa@rediris.es

Identificador del certificado (a99b99c9)  a1b33c1

PIN

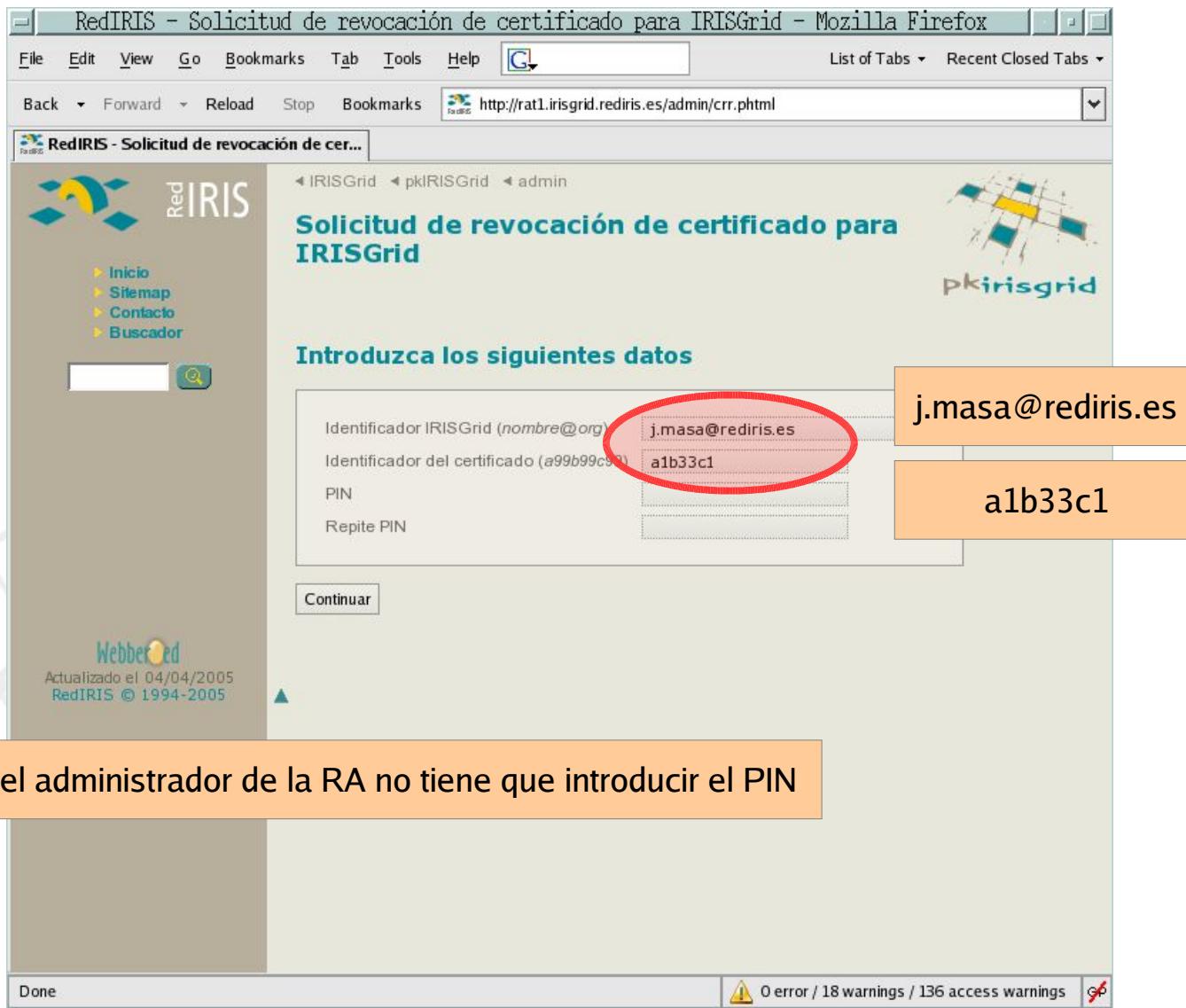
Repite PIN

Continuar

Si es el administrador de la RA no tiene que introducir el PIN

Done

0 error / 18 warnings / 136 access warnings



# PkIRISGrid v0.2 beta

## Problema al revocar un certificado inexistente

RedIRIS - Solicitud de revocación de certificado para IRISGrid - Mozilla Firefox

File Edit View Go Bookmarks Tab Tools Help

Back Forward Reload Stop Bookmarks http://rat1.irisgrid.rediris.es/admin/crr.phtml

RedIRIS - Solicitud de revocación de cer...

IRISGrid pkIRISGrid admin

Solicitud de revocación de certificado para IRISGrid

pkirisgrid

Detalles de la solicitud de revocación del certificado

Identificador IRISGrid	j.masa@rediris.es
Identificador del certificado	a1b33c1

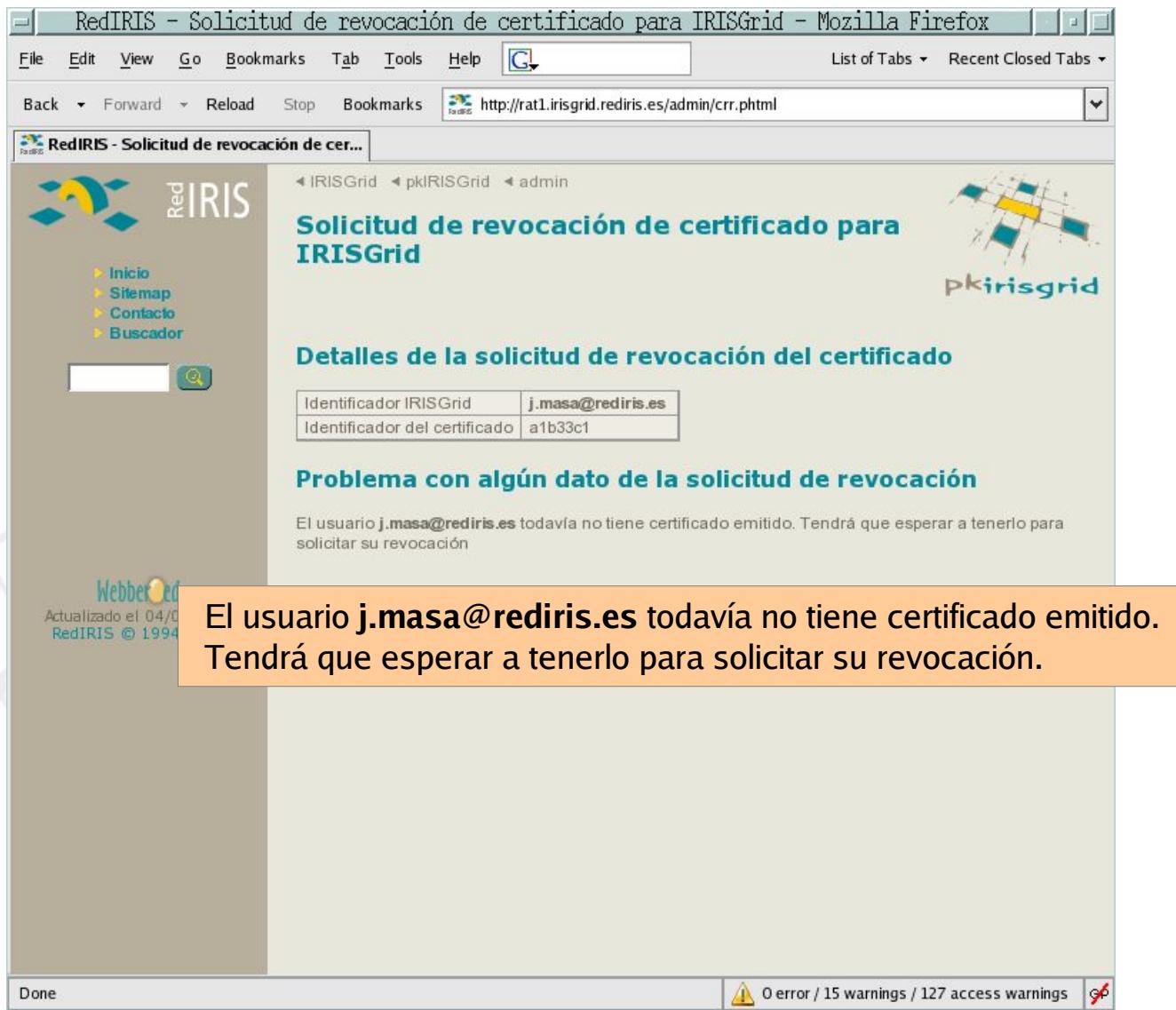
Problema con algún dato de la solicitud de revocación

El usuario j.masa@rediris.es todavía no tiene certificado emitido. Tendrá que esperar a tenerlo para solicitar su revocación.

Actualizado el 04/04/2005  
RedIRIS © 1994

Done

0 error / 15 warnings / 127 access warnings



- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura
- Tecnología usada
  - Operación
    - Capturas de pantalla
  - ¿Y ahora qué?



- **Política**
  - Vamos a desarrollar las políticas
- **Proceso de acreditación EUGridPMA**
- **Beta de pkIRISGrid**
  - Uso de la actual identidad de la CA de IRISGrid
  - Creación de varias RAs
  - Los certificados que sigan siendo válidos al finalizar la beta se refirmarán con la identidad definitiva de la CA
- **Ampliación de pkIRISGrid**
  - Vuestras sugerencias

- RA de ejemplo
  - <http://rat1.irisgrid.es>
  - <http://rat1.irisgrid.es/admin/>
- Esquema LDAP pkirisgrid
  - <http://www.rediris.es/ldap/esquemas/>
- Esta presentación estará disponible en
  - <http://www.irisgrid.es/coord/gt/gt2005/gt2005-pkirisgrid.pdf>
- Mail
  - [javier.masa@rediris.es](mailto:javier.masa@rediris.es)